REMARKS

This Amendment is submitted in full response to the outstanding Office Action of August 12, 2004, on the merits of the above-referenced application, and a request for an appropriate extension of time is enclosed herewith along with the corresponding PTO fee. Accordingly, in consideration of the amendments and remarks presented herein, re-consideration of this application is hereby respectfully requested.

In the present Office Action, claims 1-2, 5-31, 33-41, and 43-51 stand rejected under 35 U.S.C. 103(a). Specifically, claims 2, 5, and 6 are rejected as being unpatentable over Feinleib, U.S. Patent No. 6,272,532; claims 7-19, 23, and 25-30 are rejected as being unpatentable over Feinleib in view of Frailong et al., U.S. Patent No. 6,230,194; claims 20-22 are rejected as being unpatentable over Feinleib and Frailong in view of Smith et al., U.S. Patent No. 6,532,543; claims 31, 33-39, 40-41, and 43-51 are rejected as being unpatentable over Smith in view of Feinleib; claim 1 is rejected as being unpatentable over Frailong in view of Smith; and claim 24 is rejected as being unpatentable over Frailong in view of Walker et al., U.S. Patent No. 6,110,041. The Applicant notes that while the Office Action Summary indicates that claims 52-54 are also rejected, the basis for rejection of these claims is not addressed in the present Office Action.

The Applicant is once again highly appreciative of the Examiner's conscientious review of this application, and

respectfully asks for her reconsideration of same, based upon the amended and new claims presented above, and the following remarks.

A. REVIEW OF CITED REFERENCES.

In light of the bases presented for the rejection of claims, the Applicant believes that the following overview of the cited references will be helpful to clearly illustrate the distinction between Applicant's invention, as recited in the claims currently pending in the present application, and the references cited in the outstanding Office Action.

To begin, the PTO has cited U.S. Patent No. 6,272,532 issued to Feinleib (hereinafter, "Feinleib") which is directed to an electronic reminder system with universal email input. More in particular, Feinleib discloses a system which permits a message submitter to send an e-mail message to a central computer, which may comprise an e-mail server, and wherein the e-mail message includes information necessary to generate and send an electronic reminder to a specified recipient at a specified time. (column 2, lines 51-58). **Thus, inherent in the system disclosed in Feinleib, is that a communication port must remain open at the central computer to accept the e-mail message(s) transmitted by the message submitter(s), and that a direct communication pathway is required between the message submitter and the central computer.** In addition, while Feinleib discloses that the central computer may be administered, controlled and configured by e-mail commands, the

specification also indicates that the use of such "system commands" may require a passcode authentication to "reduce" tampering, thereby underscoring the fact that innovative security measures are not presented by Feinleib. (column 4, lines 11-25). Finally, Feinleib discloses a program which is executed on the central computer and is structured to perform a periodic analysis of a database which is formed of data parsed from the e-mail message(s) submitted by the message sender(s), to determine if any reminders or warnings are due to be sent, as well as to retrieve the appropriate records from the database to construct and send such reminders, preferably in the form of e-mail messages. (column 4, lines 27-38).

Next, U.S. Patent No. 6,230,194 issued to Frailong et al. (hereinafter, "Frailong") is directed to an interface for upgrading a secure network, and was cited by the PTO in the previous Office Action. The system disclosed in Frailong comprises a gateway interface device which is configured by a remote management server, either directly or indirectly. In particular, and with respect to the direct configuration of the gateway interface device, Frailong states that by providing a configuration management function within the remote management server, it is possible to download configuration and upgrade information and parameters to the gateway interface device. (column 5, lines 45-49). In addition, Frailong provides that the gateway interface device stores the configuration information transmitted from the remote management server. (column

5, lines 33-35). **Thus, from the foregoing it is clear that in order for the remote management server disclosed in Frailong to directly and remotely configure the gateway interface device a communication port must remain open at the gateway interface device to accept "configuration information transmitted from the remote management server," and a direct communication pathway is required between the remote management server and the gateway interface device.**

With regard to indirect configuration of the gateway interface device by the remote management server, Frailong further discloses that in one embodiment the remote management server sends a notification message to the gateway interface devices which are to be upgraded. The notification message includes the time an upgrade package will be made available on an FTP site, the time the upgrade is to be applied to the gateway interface device, the address of the FTP site where the upgrade is available, and a decryption key to decrypt the upgrade software. (column 15, lines 24-40). **As above, this embodiment requires that a communication port must remain open at the gateway interface device, first, to receive the notification message from the remote management server, and again to retrieve the upgrade software from the FTP site. In addition, a direct communication pathway is required, first, between the remote management server and the gateway interface device, and again between the gateway interface device and the FTP site.**

In addition, the PTO has cited U.S. Patent No. 6,532,543 issued to Smith et al. (hereinafter, "Smith") which is directed to a system and method for installing an auditable secure network. Smith discloses a system including a remote computer having an electrical connection, such as TCP/IP, to a network, such as the internet. In one embodiment, Smith discloses a system to permit a user of a remote computer to purchase a software application from a content server via the internet. (column 9, lines 13-21). In this embodiment, the billing and user information are transmitted using secure methods, such as encoding the information in a manner only readable by a server module, or a key-escrow encapsulated within an application program interface ("API"), such as a Secure Socket Layer ("SSL") in Netscape, or Microsoft's CRYPTOAPI. Regardless of the coding or encryption methodology, the server module transmits an enabling command which allows the software program to be transmitted to the remote computer. **As with the preceding references, this embodiment of Smith requires that a communication port must remain open on the remote computer to receive the software application transmitted from the content server, and a direct communication pathway is required between the remote computer and the content server.**

Smith also discloses a system for generating, installing, and maintaining a secure network, including a plurality of application nodes. (column 16, lines 50-53). Smith provides that while the communication between nodes, between servers, and between servers

and nodes may be accomplished using any of a variety of communication links and protocols, it is preferably accomplished using TCP/IP. Further, Smith discloses that when a node is run on a target site, it includes capability to automatically connect with a monitor node (column 22, lines 55-57), and further that the monitor node communicates with each other node in the network to which a node being installed is to be linked, and updates the other nodes with information relating to the node being installed to prepare the other nodes to connect with the node being installed. (column 24, lines 2-7). Smith also discloses an elaborate methodology for "strobing" of the encryption means between nodes, wherein encryption and SSL connections are relied upon to maintain the security of the network. **Once again, however, this embodiment of the invention disclosed by Smith inherently requires that a communication port must remain open on each node to permit the "strobing" process to occur, and a direct communication pathway is required between nodes to facilitate the "strobing" process.**

Finally, U.S. Patent No. 6,110,041 issued to Walker et al. (hereinafter, "Walker") has been cited, Walker being directed to a method and system for adapting gaming devices to playing preferences. More in particular, Walker discloses a slot network server and a slot machine structured to transmit digitally encoded data and messages to one another, such as player name and identification number, authenticated player identification and preferences selections. Walker also discloses a communication

port, like other conventional server computers, which connects the slot network server to an interface which links the slot network server to the slot machine. (column 4, lines 17-24). Specifically, Walker provides for a player to transmit selected preference information to the slot network server (column 7, lines 56-60); for the slot network server to transmit data or codes representing player preferences to the slot machine for the slot machine to configure the game to match player preferences (column 8, lines 11-30); and to transmit data or codes representing the casino preferences to the slot machine for the slot machine to configure the game in accordance with casino preferences. (column 8, lines 51-59). **As with the foregoing references cited by the PTO, the invention disclosed by Walker requires that a communication port must remain open on both the slot network server and the slot machine to facilitate the exchange of data and/or codes required to reconfigure each slot machine, and a direct communication pathway is required between the slot network server and the slot machine.**

Conversely, in the present invention, no communication port remains open on a remote site to receive a transmission from an administration site. Thus, the present invention eliminates the security risk inherent in having a communication port remain open, which provides an accessible point of entry to the system by hackers. ***Additionally, in the present invention no direct communication pathway is required between the administration site***

and the gateway site, by virtue of a remote staging platform. This further eliminates potential points of entry to both the administration and the gateway sites through which hackers may once again readily access the system. Specifically, in one preferred embodiment, the invention of the present application comprises an administrative site structured to transmit encoded configuration data to a remote staging platform, such as a remote e-mail server, and a gateway server structured to poll the remote staging platform for a message specifically directed to the gateway server, thereby establishing an indirect communication pathway between the administration site and the gateway server. The gateway server of the present invention is structured to retrieve the message (i.e. the encoded configuration data) from the remote staging platform via standard e-mail protocols, such as SMTP, thereby eliminating the need for the gateway server to have a port remain open to retrieve the configuration data, as well as providing an indirect communication link between the administration server and the gateway server. ***Thus, in the present invention, no communication port remains open on the gateway server to receive transmission of configuration data from an outside source, such as the administration site. In addition, the need for a secure connection to transmit configuration data, such as SSL or CRYPTOAPI, is eliminated by way of the indirect communication pathway between the administration site and the gateway server via the remote staging platform.***

B. Amended Independent Claims 1, 2, 31, 41, and 52.

In view of the foregoing, the Applicant has amended each of previously presented independent claims to specifically recite that no port remains open at the gateway server, the initialized device or the networked device to receive a file or configuration data. This recitation is fully supported by the specification as originally filed in the present application (see page 7, lines 1-2; page 8, lines 6-7; and page 8, lines 13-15).

Thus, the Applicant respectfully asserts that the invention recited in each of the independent claims as amended herein, namely, claims 1, 2, 31, 41, and 52, is new, novel and non-obvious in view of the references cited by the PTO, and each of these claims are, therefore, in condition for immediate allowance. Additionally, each of the original or previously presented dependent claims remaining in the present application are either directly or indirectly dependent on one of the currently amended independent claims and are now also in condition for immediate allowance. The Applicant submits that the currently amended claims are fully supported by the disclosure of the specification as originally filed in the present application, as noted above, and do not contain new matter.

C. New Claims 55-56.

The Applicant presents herein new independent claim 55 which specifically recites an embodiment of the present invention

wherein, once again, "no port remains open at the at least one networked device to retrieve the configuration data file." Thus, for the reasons presented above, the Applicant believes this claim is also in condition for immediate allowance. In addition, the Applicant submits that new dependent claim 56, which depends directly from new independent claim 55 is, thus, also in condition for immediate allowance. The Applicant submits that new claims 55 and 56 are fully supported by the disclosure of the specification as originally filed in the present application, and as noted above, and do not contain new matter.

D. <u>New Claims 57-58</u>.

The Applicant further presents herein new independent claim 57, which recites an embodiment of the present invention "wherein a direct communication pathway is not required between the administration site and the at least one networked device to retrieve the configuration data file." This recitation is fully supported by the specification as originally filed in the present application (see page 6, lines 23-29; and page 7, lines 19-22). Thus, the Applicant respectfully asserts that the invention recited in new independent claim 57 is new, novel and non-obvious in view of the references cited by the PTO, and this claim is, therefore, in condition for immediate allowance. In addition, the Applicant submits that new dependent claim 58, which depends directly from new independent claim 57 is, thus, also in condition for immediate

allowance. The Applicant submits that new claims 57 and 58 are fully supported by the disclosure of the specification of the present application, as noted above, and do not contain new matter.

Accordingly, based on the above Amendments and Remarks, the Examiner is respectfully requested to reconsider her position with regard to the present application. Since nowhere in the art is this new, novel and non-obvious invention found, taught, or suggested, it is urged that this case is now clearly in condition for allowance and, accordingly, such action is respectfully solicited.

In the event that any fee may be required by the filing of this paper, an Authorization to Charge Fees to Deposit Account, **Deposit Account No. 13-1227**, is being filed concurrently with this Amendment. Please note that our docket number related to this matter is **1.300.04**.

Respectfully submitted,

MALLOY & MALLOY, P.A.
Attorneys for Applicant
2800 S.W. Third Avenue
Historic Coral Way
Miami, Florida 33129
(305) 858-8000

By: John Fulton Jr.
John Fulton, Jr.
Reg. No. 46,716

Dated: 11-23-04